REMARKS

In response to the Final Office Action dated 1/13/2005, applicant requests withdrawal of the holding of finality under 37 CFR 1.114. Applicant also requests withdrawal of the appeal (notice of which was given on 3/1/2005) and re-opening of the prosecution of the application before the Examiner.

An IDS citing Driscoll, III et al. (US 6,044,405) is included herewith. Driscoll was cited in US patent application 09/596,857 that is directed toward pricing a cryptographic service.

Included herewith is an authorization for a two month extension of time which will end on 6/13/05.

Claims 1, 2, 13, 14 and 20 were amended. Claim 1 was amended to more clearly point out that the server that performs the cryptographic service receives a second key (the second key being a private key) over the tunnel and uses that key to perform the cryptographic service. Independent claims 13 and 20 were similarly amended. Claims 2 and 14 were amended to be consistent with the amendments made in their respective parent claims. These amendments are supported by Fig. 6 page 18, lines 12-21 (amended in the office action reply sent 6/19/2000), page 2, line 12 to page 3, line 6, page 3, line 19-page 4, line 2; and the application as a whole.

During the preparation of an appeal brief for this application, applicant received an office action for US patent application 09/596,857, which is directed toward pricing a cryptographic service, and that cited Driscoll, III et al. (US 6,044,405). Based on this citation, applicant determined that continuing with the appeal on the instant case would be moot because, even if applicant succeeded at the appeal, Driscoll would be cited against the previous claims. Applicant has amended claims 1, 2, 13, 14 and 20 accordingly.

Driscoll teaches a method for conveying large blocks of data between geographically-remote locations through hub sites, invoicing for this service, and having the hub site provide value added services. One of the value-added services mentioned in Driscoll is encryption. However, none of the details required to successfully implement a cryptoserver are disclosed.

Nothing in Driscoll teaches a cryptographic service that identifies a client, establishes a first key, generates a tunnel on the network, receives a second key at the server from the client over the tunnel where the second key is a private key of a key pair that is encrypted by the first key, and uses the second key at the server to perform the cryptographic service to off load the computational burden associated with the cryptographic service from the client.

I. General Comments regarding the claimed invention

The currently claimed invention is directed towards a **cryptographic service.** The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22 (as well as the application as a whole).

To summarize, a cryptographic service provider operates a server. The server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the server that provides the service of performing the cryptographic operation. One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a server that performs the requested cryptographic service for the client.

The server thus provides a cryptographic service to a client computer such that the client computer can off-load the computational burden due to cryptographic operations from the client computer to the cryptographic server. The cryptographic operations performed by the server are those that could have been performed by the client.

The invention of currently amended claim 1 is directed to a networked server that provides a cryptographic service. The method includes the following steps.

(a) identifying a client utilizing the network;

(b) establishing a first key;

(c) generating a tunnel on the nctwork;

(d) receiving a second key at the server from the client utilizing the tunnel, wherein the second key is encrypted by the client using the first key, the second key being a private key of a key pair; and

(e) performing the cryptographic service at the server for thc client, the server using the second key to perform the cryptographic service, whereby the server off-loads a computational burden associated with the cryptographic service from thc client.

Thus, the claimed invention is directed to providing a cryptographic service from a networked server where the networked server receives a private key of a key pair over the tunnel and uses the private key to perform the cryptographic service, thus off-loading the computational burden associated with the cryptographic service from the client computer to the server computer.

III. Rejections under 35 USC §103(a)

Claims 1-3, 5-15 and 17-22 stand rejected under 35 USC §103(a) as being unpatentable over McGarvey (6,643,774) in view of Kirby (5,898,784).

A prima facie case of obviousness is established when the Examiner provides one or more referencds that were available to the inventor and that teach a suggestion to combine or modify the references the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

With rcgards to McGarvey: McGarvey teaches techniques for allowing a server to use a client computer's (or user's) authority so that the server computer can access protected resources or perform protected services on behalf of the client (McGarvey column 2, lines 4-11; column 6, line 64 – column 7 line 16; and column 8, lines 52-56). McGarvey also teaches a public key system using public/private key pairs (column 1, line 56-column 2, line 11).

The problem addressed by McGarvey is how to allow a client computer to give a server the same access to protected data or services that the client has. It does this by delegating client authority to a server so that the server can access the protected data or services in place of the client. This delegation is accomplished by using a public key encryption system to establish trusted communication between a client, a server, and a private key system.

Nothing in McGarvey teaches to one skilled in the art a suggestion to modify McGarvey to send the client's private key of a key pair to a server to perform the cryptographic service using the client's private key.

With regards to Kirby: Kirby teaches network tunneling and encryption techniques.

The problem addressed by Kerby is that of sending network packets through firewalls.

While Kirby recognizes the burden of encrypting and decrypting packets (Kirby: column 6, lines 25-40), Kirby suggests spreading the burden to multiple computers by terminating the virtual tunnels at the different computers.

Thus, nothing in Kirby teaches to one skilled in the art a suggestion to modify Kirby to include a networked server that provides cryptographic services to a client. Furthermore, nothing in Kirby teaches a suggestion to send the client's private key of a key pair to a server to perform the cryptographic service using the client's private key

Nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to a networked server that provides cryptographic services to a client using the client's private key of a key pair.

Thus, currently amended **claim 1** is patentable. Currently amended **claim 13** and currently amended **claim 20** are a program product claim and a system claim (respectively) that are comparable with currently amended claim 1 and so are also patentable for the same reasons.

Currently amended claims 2 and 14 depend on and further limit their respective independent claims that are patentable and thus claims 2 and 14 are also patentable.

Previously presented claims 3 and 15 depend on and further limit their respective parent claims that are patentable and thus claims 3 and 15 are also patentable.

Previously presented claim 21 depends on and further limits patentable claim 3 and thus claim 21 is also patentable.

Claims 4 and 16 have been previously canceled.

Previously presented claims 5 and 17 depend on and further limit their respective independent claims that are patentable and thus claims 5 and 17 are patentable. Furthermore, nothing in McGarvey or Kirby, separately or combined, teach a suggestion that would lead one skilled in the art to off-load modular exponentiation from a client to a cryptographic server.

Previously presented claims 6 and 18 depend on and further limit their respective independent claims that are patentable. Thus claims 6 and 18 are also patentable.

Original claim 22 depends on and further limits patentable claim 21 and thus claim 22 is also patentable.

Previously presented claims 7-9 and 19; and original claims 10-12 depend on and further limit their respective parental claims that are patentable. Thus, claims 7-9, 10-12 and 19 are patentable.

The undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No.

24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,

DANIEL B. CURTIS
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com